Grandstream Device Management System (GDMS) Privacy Statement: How GDMS Processes User Data

Updated: March 22, 2022

This privacy statement discloses security and privacy information related to the processing of data by Grandstream Device Management System (GDMS). GDMS is a cloud management platform for managing, provisioning, and monitoring supported Grandstream products. This document is supplemental to Grandstream Privacy Statement.

Device Data Reporting Content, Period and Security Processing

Devices managed by GDMS communicate with the cloud service via the TR-069 protocol. All communication except for UDP packets is processed over HTTPS connection encrypted using TLS v1.2.

The following information is periodically reported to GDMS by added devices:

1. Device MAC address
   UDP keep-alive packets are used to monitor and maintain the connection between a device and GDMS and to trigger the TR-069 process. Data sent to GDMS contains only the MAC address of the connected device. These UDP packets are sent in intervals of 15-45 seconds depending on the network connection quality of the device.

2. Device basic information and network information
   Device basic information and network information include device model, MAC address, firmware version, hardware version, private network, public network information, etc.
   The device basic information and network information are reported periodically based on the TR-069 standard process. Usually, the device reports basic information and network information on a daily basis or longer. Under extremely poor network conditions, the minimum reporting interval could be as short as 5 minutes. The actual interval will be dynamically regulated by the GDMS platform according to the network condition of the device.

3. Account registration status
   Listening events such as address and port changes will be triggered if the device has account status and network condition updates.

4. UCM statistics data
   GDMS collects information reported daily from added UCM IPPBX devices to generate statistical data such as the model, the number of registered extensions, the number of end devices, call duration, etc…
5. UCM plan information

UCM device retrieves RemoteConnect plan information from GDMS daily. UCM does not report any plan information itself to GDMS.

6. Other data
   Data such as device call quality, user operations including viewing device information, synchronizing device configuration, capturing Syslog, diagnosis and etc… is reported only when the related tasks are scheduled on GDMS. GDMS does not actively request the data.

Obtaining Device Status and User Data Privacy

After the user adds a device to GDMS, GDMS will obtain the device status. The device status in GDMS is solely based on the UDP keep-alive packets. GDMS does not monitor or collect devices' call status information.

GDMS is capable of processing call quality reports from supported devices, which include MOS, packet loss rate, jitter, and latency. This information is not collected and processed by default, and users would need to manually enable the option in GDMS. To take advantage of this feature, supported devices would need to be both added to GDMS and registered to a UCMRC server address. Collected data does not include the audio and video content of calls and is solely for the purpose of calculating and displaying statistics on the GDMS portal.

Device Provisioning and Security

GDMS does not retrieve the device configuration information of added devices and will not provision any settings unless explicitly selected by the GDMS user. All settings that can be provisioned to devices from GDMS are visible on the GDMS portal. During the provisioning process, communication with the target device(s) is encrypted via TLS 1.2 to protect user data.

Legal Basis for Data Processing

GDMS is GDPR compliant, and data stored in its US and EU servers are managed separately.

Except for user login credentials, channel devices, and relationship information for the channels, data stored in the US server's database is not shared with the EU servers, and vice versa. Account login information, channel devices, and channels' relationship information are stored in a centralized database. Sensitive user data is not included in the information mentioned above.

Permission Management

On GDMS, data owned by different enterprises are isolated from each other. The data managed by different users are restricted to the assigned user's role and permission. Grandstream GDMS technical support does not have permission to manage users' devices unless the user authorizes specific devices to Grandstream.

On GDMS, an enterprise's data is not shared with any other enterprise unless the user authorizes it. Users can only view and manage data that their assigned permissions allow them to. Grandstream GDMS technical support does not have permission to manage user devices unless specifically authorized by the user to Grandstream.

Data Storage

1. Grandstream devices fully compatible with GDMS will initiate a connection to GDMS by default, minimizing the amount of configuration users will need to do to successfully add their devices to GDMS. Devices not added to GDMS will have their MAC address data encrypted and stored in the regional server's database. Public network addresses and other device information are not stored for data security purposes.

2. GDMS does not store user passwords in plaintext format. Passwords are hashed before storage and cannot be decrypted to protect user privacy.

3. After the user adds a device to GDMS, the device serial number is encrypted and stored in the GDMS regional server database. GDMS does not store a device's factory password.

4. After the user adds a UCM device to GDMS, UCM can back up its configuration, CDR, and IM data to GDMS cloud storage. Backup files are encrypted and cannot be read or modified directly by users for security purposes.

UCMRC Services

As a proxy server, the UCMRC service provides external network penetration ability for UCM and forwards media streams data between UCM and their SIP endpoints/Wave clients. For UCM with UCMRC service, the end-to-end communication between UCM and their SIP endpoints/Wave clients is encrypted via TLS v1.2, and the media stream is encrypted in SRTP using the AES algorithm. UCMRC service will not process or store the transmitted data between UCM and any terminals, nor intercept or analyze any communication data from users. Users' privacy and data security are fully protected.